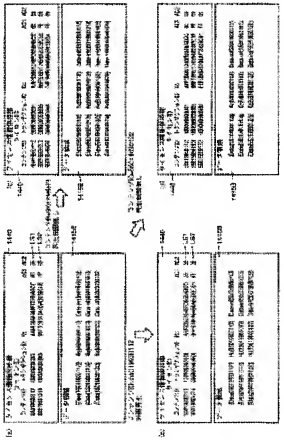
DATA TERMINAL EQUIPMENT

Publication number: JP2002091827 (A)
Publication date: 2002-03-29
Inventor(s): HORI YOSHIHIRO
Applicant(s): SANYO ELECTRIC CO
Classification:
- international: ***G06F12/14; G06F12/00; G06F21/24; G06Q30/00; G10K15/02;*** **G06F12/14; G06F12/00; G06F21/00; G06Q30/00; G10K15/02;** (IPC1-7): G06F12/14; G06F12/00; G06F17/60
- European:
Application number: JP20000284862 20000920
Priority number(s): JP20000284862 20000920

Abstract of **JP 2002091827 (A)**

PROBLEM TO BE SOLVED: To provide portable terminal equipment for receiving only required enciphered contents data and/or license key or the like from a distribution server. SOLUTION: When the receiving request of enciphered contents data Data} Kc is inputted from a user, a portable telephone set retrieves the recording conditions of a contents ID, license key Kc, reproducing time limit information AC1, reproducing time limit and enciphered contents data Data}Kc or the like on a loaded memory card. Then, only the enciphered contents data Data}Kc and license (contents ID, license key Kc, reproducing time limit information AC1 and reproducing time limit), which are not recorded in a license area 1415A and a data area 1415B of the memory card are received from the distribution server.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－91827
（Ｐ2002－91827Ａ）
(43)公開日　平成14年３月29日(2002.3.29)

(51)Int.Cl.⁷		識別記号	Ｆ Ｉ			ﾃｰﾏｺｰﾄﾞ（参考）
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ	５Ｂ０１７
	12/00	５３７		12/00	５３７Ｈ	５Ｂ０４９
	17/60	３０２		17/60	３０２Ｅ	５Ｂ０８２

審査請求　未請求　請求項の数14　ＯＬ　（全 31 頁）

(21)出願番号　特願2000－284862(Ｐ2000－284862)

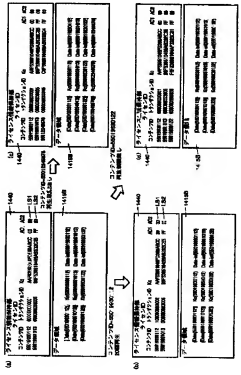
(22)出願日　平成12年９月20日(2000.9.20)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

Ｆターム(参考)　５Ｂ０１７ ＡＡ０７ ＢＡ０７ ＢＢ０７ ＣＡ１６
５Ｂ０４９ ＡＡ０５ ＡＡ０６ ＥＥ０５ ＦＦ０１ ＦＦ０８
ＧＧ００
５Ｂ０８２ ＧＡ１１

(54)【発明の名称】　データ端末装置

(57)【要約】
【課題】　必要な暗号化コンテンツデータおよび／またはライセンス鍵等のみを配信サーバから受信する携帯端末装置を提供する。
【解決手段】　携帯電話機は、ユーザから暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの受信要求が入力されると、装着されたメモリカードにおけるコンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限情報ＡＣ１、再生期限、および暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ等の記録状況を検索する。そして、メモリカードのライセンス領域１４１５Ａ、データ領域１４１５Ｂに記録されていない暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス（コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限情報ＡＣ１、再生期限）だけを配信サーバから受信する。



【特許請求の範囲】

【請求項１】　コンテンツデータを暗号化した暗号化コンテンツデータおよび／または前記暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、前記暗号化コンテンツデータおよび／または前記ライセンスを記録するデータ端末装置であって、

前記暗号化コンテンツデータおよび前記ライセンスを記録するデータ記録部と、

外部との通信を行なう送受信部と、

前記データ記録部とのデータ授受を制御するインタフェースと、

指示を入力するためのキー操作部と、

制御部とを備え、

前記制御部は、前記キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータが前記データ記録装置に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生することができるライセンスの有無を検索し、

前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、および／または前記ライセンスが無いとき、前記暗号化コンテンツデータおよび／または前記ライセンスの配信を前記送受信部を介して配信サーバへ要求する、データ端末装置。

【請求項２】　前記制御部は、前記送受信部が前記配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、前記暗号化コンテンツデータおよび／または前記ライセンスの検索を行なう、請求項１に記載のデータ端末装置。

【請求項３】　前記受信要求する暗号化コンテンツデータの決定は、前記メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツＩＤが選択されることによって行なわれ、

前記制御部は、前記選択されたコンテンツＩＤに基づいて前記暗号化コンテンツデータおよび／または前記ライセンスの検索を行なう、請求項２に記載のデータ端末装置。

【請求項４】　前記制御部は、前記暗号化コンテンツデータの検索を行ない、前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、前記暗号化コンテンツデータの配信を前記送受信部を介して前記配信サーバへ要求する、請求項１から請求項３のいずれか１項に記載のデータ端末装置。

【請求項５】　前記制御部は、前記暗号化コンテンツデータが前記データ記録装置に記録されているとき、前記ライセンスの検索を行なう、請求項４に記載のデータ端末装置。

【請求項６】　前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、

前記制御部は、受信要求された暗号化コンテンツデータが前記データ記録部に記録されており、前記ライセンス鍵および前記再生制限情報が前記データ記録部に記録されていないとき、前記ライセンスが無いと判断する、請求項１に記載のデータ端末装置。

【請求項７】　前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、

前記制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵が前記データ記録部に記録されており、前記暗号化コンテンツデータの再生が前記再生制限情報によって制限されているとき、前記ライセンスが無いと判断する、請求項１に記載のデータ端末装置。

【請求項８】　前記制御部は、前記キー操作部から入力された変更後の再生制限情報を前記ライセンスの購入条件として前記コンテンツＩＤとともに前記送受信部を介して前記配信サーバへ送信する、請求項７に記載のデータ端末装置。

【請求項９】　表示部をさらに備え、

前記制御部は、前記メニュー情報を前記表示部に表示し、ユーザが前記表示部に表示された前記メニュー情報に基づいて前記コンテンツＩＤを選択するための情報をキー操作部を介して入力することによって、前記コンテンツＩＤを取得する、請求項３に記載のデータ端末装置。

【請求項１０】　前記メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、

前記表示部は、前記移行情報を入力するための入力部を含み、

前記制御部は、前記入力部から前記移行情報が入力されると、前記移行情報に基づいて決定される他の画面を前記表示部に表示する、請求項９に記載のデータ端末装置。

【請求項１１】　前記制御部は、前記ライセンスの購入条件と、前記インタフェースを介して取得した前記データ記録部の認証データおよび前記コンテンツＩＤとを前記送受信部を介して前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証された場合のみ、前記ライセンスを受信する、請求項１から請求項１０のいずれか１項に記載のデータ端末装置。

【請求項１２】　前記ライセンスに従って前記暗号化コンテンツデータを再生するデータ再生部をさらに備え、

前記制御部は、前記キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報と前記暗号化コンテンツデ

ータとを前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える、請求項１から請求項１１のいずれか１項に記載のデータ端末装置。

【請求項１３】　前記バスに接続され、前記データ記録部に対する認証データを保持する認証データ保持部をさらに備え、

暗号化コンテンツデータの再生時、

前記制御部は、前記認証データが前記データ記録部において認証された場合のみ前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報を前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える、請求項１２に記載のデータ端末装置。

【請求項１４】　前記データ記録部は、着脱可能なデータ記録装置である、請求項１から請求項１３のいずれか１項に記載のデータ端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータを配信サーバから受信するとき、携帯電話機は、暗号化コンテンツデータとともに暗号化コンテンツデータを復号するライセンス鍵、および暗号化コンテンツデータの再生回数、再生期限等を設定した購入条件を配信サーバから受信し、メモリカードに記録する。

【００１５】また、携帯電話機は、暗号化コンテンツデータを再生するとき、暗号化コンテンツデータの再生が受信した再生回数、再生期限等によって制限されないときに暗号化コンテンツデータを再生する。

【００１６】さらに、携帯電話機は、配信サーバ以外から暗号化コンテンツデータのみを受信し、メモリカードに記録する場合もある。

【００１７】したがって、暗号化コンテンツデータがメモリカードに記録されているが、ライセンス鍵がメモリカードに記録されていない場合、暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されているが、再生回数、再生期限等によって暗号化コンテンツデータの再生が制限される場合、および暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されていない場合等が想定される。

【００１８】かかる場合に、ユーザから暗号化コンテンツデータの配信要求がされた場合、直ちに配信サーバへ暗号化コンテンツデータおよびライセンス鍵等の配信を要求したのでは、同じ暗号化コンテンツデータおよびライセンス鍵を配信サーバから受信することになり、同じ暗号化コンテンツデータに対して料金を複数回支払うという問題が生じる。

【００１９】また、暗号化コンテンツデータを配信サーバから受信するために不要な時間を必要とするという問題もある。

【００２０】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、必要な暗号化コンテンツデータおよび／またはライセンス鍵等のみを配信サーバから受信するデータ端末装置を提供することである。

【００２１】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび／または暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、暗号化コンテンツデータおよび／またはライセンスを記録するデータ端末装置であって、暗号化コンテンツデータおよびライセンスを記録するデータ記録部と、外部との通信を行なう送受信部と、データ記録部とのデータ授受を制御するインタフェースと、指示を入力するためのキー操作部と、制御部とを備え、制御部は、キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータがデータ記録部に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生するためのライセンスの有無を検索し、暗号化コンテンツデータがデータ記録部に記録されていないとき、および／またはライセンスが無いとき、暗号化コンテンツデータおよび／またはライセンスの配信を送受信部を介して配信サーバへ要求する。

【００２２】この発明によるデータ端末装置においては、ユーザから暗号化コンテンツデータの受信要求がキー操作部を介して入力されると、制御部は、受信要求がなされた暗号化コンテンツデータおよび／またはライセンスがデータ記録部に記録されているか否かを検索し、データ記録部に記録されていない暗号化コンテンツデータおよび／またはライセンスの配信を配信サーバへ要求する。つまり、データ端末装置は、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況に応じて必要な暗号化コンテンツデータおよびライセンスだけを配信サーバから受信し、かつ、データ記録部に記録する。

【００２３】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの重複記録を防止できる。

【００２４】また、この発明によれば、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。

【００２５】さらに、この発明によれば、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【００２６】好ましくは、データ端末装置の制御部は、送受信部が配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【００２７】データ端末装置は、配信サーバから受信したメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【００２８】したがって、この発明によれば、受信要求された暗号化コンテンツデータおよびライセンスがデータ記録部に記録されているか否かを正確に判断できる。

【００２９】好ましくは、受信要求する暗号化コンテンツデータの決定は、メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツＩＤが選択されることによって行なわれ、制御部は、選択されたコンテンツＩＤに基づいて暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【００３０】ユーザは、暗号化コンテンツデータのコンテンツＩＤを特定することによって受信要求する暗号化コンテンツデータを選択する。そうすると、データ端末装置の制御部は、選択された暗号化コンテンツデータのコンテンツＩＤを抽出し、その抽出したコンテンツＩＤに基づいて、暗号化コンテンツデータおよび／またはライセンスがデータ記録部に記録されているか否かを検索する。

【００３１】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよび／またはライセンスの検索を正確に行なうことができる。

【００３２】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、暗号化コンテンツデータの配信を送受信部を介して配信サーバへ要求する。

【００３３】データ端末装置の制御部は、コンテンツＩＤを用いてデータ記録部における暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、データ記録部におけるライセンスの検索を行なうわずに暗号化コンテンツデータおよびライセンスの配信を配信サーバへ要求する。

【００３４】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況を迅速に検索し、その記録状況に応じて必要な暗号化コンテンツデータおよびライセンスを配信サーバから受信できる。

【００３５】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されているとき、ライセンスの検索を行なう。

【００３６】データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されていないことを確認した後に、ライセンスの検索を行なう。

【００３７】したがって、この発明によれば、必要な検索のみを行なうことによって検索時間を短縮し、かつ、正確な検索を行なうことができる。

【００３８】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータがデータ記録装置に記録されており、ライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、ライセンスが無いと判断する。

【００３９】ライセンスを構成するライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在したいと判断する。

【００４０】したがって、この発明によれば、データ記録部に暗号化コンテンツデータのみが記録されているとき、ライセンス鍵および再生制限情報を配信サーバから受信することができる。

【００４１】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵がデータ記録部に記録されており、暗号化コンテンツデータの再生が再生制限情報によって制限されているとき、ライセンスが無いと判断する。

【００４２】ライセンスを構成する再生制限情報のみがデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在しないと判断する。

【００４３】したがって、この発明によれば、再生制限情報のみがデータ記録部に記録されていないとき、再生制限情報を配信サーバから受信してライセンスを取得することができる。

【００４４】好ましくは、データ端末装置の制御部は、キー操作部から入力された変更後の再生制限情報をライセンスの購入条件としてコンテンツＩＤとともに送受信部を介して配信サーバへ送信する。

【００４５】データ端末装置の制御部は、再生制限情報のみを変更することによって暗号化コンテンツデータの購入条件が設定されると、コンテンツＩＤとともに設定された購入条件を配信サーバへ送信する。そして、データ端末装置は、再生制限情報を配信サーバから受信し、データ記録部に記録する。

【００４６】したがって、この発明によれば、ライセンスを購入して暗号化コンテンツデータを再生し、ライセンスが無くなった場合にも新たに再生制限情報だけを配信サーバから購入することによって暗号化コンテンツデータを再生することができる。

【００４７】好ましくは、データ端末装置は、表示部をさらに備え、制御部は、メニュー情報を表示部に表示し、ユーザが表示部に表示されたメニュー情報に基づいてコンテンツＩＤを選択するための情報をキー操作部を介して入力することによって、コンテンツＩＤを取得する。

【００４８】配信サーバから配信されたメニュー情報は、データ端末装置の表示部に表示される。そして、ユーザは表示部に表示されたメニュー情報を見て受信を希望する暗号化コンテンツデータのコンテンツＩＤを選択するための情報をキー操作部から入力する。そうすると制御部は、キー操作部を介して選択されたコンテンツＩＤを取得する。

【００４９】したがって、この発明によれば、ユーザは視覚情報に基づいて受信を希望する暗号化コンテンツデータを決定できる。また、この発明によれば、コンテンツＩＤを選択するための情報が入力されるので、制御部

は、選択されたコンテンツＩＤに基づいて、暗号化コンテンツデータおよび／またはライセンスの検索を迅速に行なうことができる。

【００５０】好ましくは、メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、表示部は、移行情報を入力するための入力部を含み、制御部は、入力部から移行情報が入力されると、移行情報に基づいて決定される他の画面を表示部に表示する。

【００５１】データ端末装置の表示部に表示されたメニュー情報に受信を希望する暗号化コンテンツデータが含まれていないとき、ユーザは移行情報を入力する、そうすると、データ端末装置の制御部は、次の画面に移行し、新たなメニュー情報を表示部に表示する。

【００５２】したがって、この発明によれば、多くの暗号化コンテンツデータの中から受信を希望する暗号化コンテンツデータを選択できる。

【００５３】好ましくは、データ端末装置の制御部は、ライセンスの購入条件と、インタフェースを介して取得したデータ記録部の認証データおよびコンテンツＩＤとを送受信部を介して配信サーバへ送信し、配信サーバにおいて認証データが認証された場合のみ、ライセンスを受信する。

【００５４】配信サーバがデータ記録部から送られてきた認証データを認証した場合のみ、データ端末装置はライセンスを受信する。

【００５５】したがって、この発明によれば、正規なデータ記録部にだけライセンスを与えることができる。その結果、暗号化コンテンツデータの保護を図ることができる。

【００５６】好ましくは、データ端末装置は、ライセンスに従って暗号化コンテンツデータを再生するデータ再生部をさらに備え、制御部は、キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報と暗号化コンテンツデータとをデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータおよび必要な情報をデータ再生部に与える。

【００５７】暗号化コンテンツデータの再生時、制御部は、ライセンスを構成する種々の情報のうち、再生に必要な情報だけをデータ記録部から取出し、暗号化コンテンツデータと、再生に必要な情報とをデータ再生部に与える。そして、データ再生部は、必要な情報によって暗号化コンテンツデータを復号および再生する。

【００５８】したがって、この発明によれば、再生に必要な情報によって暗号化コンテンツデータの再生を制限することができる。

【００５９】好ましくは、データ端末装置は、データ記録部に対する認証データを保持する認証データ保持部をさらに備え、暗号化コンテンツデータの再生時、制御部は、認証データがデータ記録部において認証された場合のみ暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報をデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータをデータ再生部に与える。

【００６０】配信サーバから受信した暗号化コンテンツデータを再生するとき、データ記録部に対するデータ端末装置の正当性が確認された場合だけ、データ端末装置はデータ記録部から暗号化コンテンツデータを受取り、暗号化コンテンツデータを再生する。

【００６１】したがって、この発明によれば、正規なデータ端末装置だけが暗号化コンテンツデータを再生できる。その結果、暗号化コンテンツデータの不法なコピー等を防止して保護を図ることができる。

【００６２】好ましくは、データ記録部は、データ端末装置から着脱可能なデータ記録装置である。

【００６３】データ端末装置は、配信サーバから暗号化コンテンツデータおよびライセンスを受信すると、その受信した暗号化コンテンツデータおよびライセンスを着脱可能なデータ記録装置へに記録する。

【００６４】したがって、この発明によれば、複数のデータ記録装置に暗号化コンテンツデータおよび／またはライセンスを記録することができる。

【００６５】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００６６】図１は、本発明による携帯端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００６７】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００６８】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０で

ある携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【００６９】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

【００７０】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００７１】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００７２】以下では、このようなライセンスサーバ１０と配信キャリア２０と併せて、配信サーバ３０と総称することにする。

【００７３】また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００７４】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００７５】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００７６】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００７７】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００７８】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００７９】まず、配信サーバ３０より配信されるデータについて説明する。Ｄａｔａは、音楽データ等のコンテンツデータである。コンテンツデータＤａｔａには、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

【００８０】なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００８１】さらに、配信サーバ３０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、配信サーバ３０からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ３０と携帯電話機１００との間でやり取りされる。さらに、ライセンス情報としては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）のアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１およびデータ再生端末における制御情報である再生期限ＡＣ２等が存在する。以後、ライセンス鍵ＫｃとコンテンツＩＤとライセンスＩＤと再生回数期限ＡＣ１と再生期限ＡＣ２とを併せて、ライセンスと総称することとする。

【００８２】図３は、図１に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【００８３】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００８４】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリス

トデータＣＲＬが含まれる。

【００８５】禁止クラスリストデータＣＲＬは、配信サーバ３０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から受取った禁止クラスリストの更新の有無を判断し、更新されていないとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データＣＲＬ＿ｄａｔを配信サーバ３０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬが書替えられる構成とするも可能である。また、禁止クラスリストのバージョンについては、ＣＲＬ＿ｖｅｒをメモリカード側より出力し、これを配信サーバ３０側で確認することによってバージョン管理を実行する。差分データＣＲＬ＿ｄａｔには新たなバージョンの情報も含まれる。

【００８６】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードへのライセンス鍵の供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【００８７】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【００８８】携帯電話機およびメモリカードには固有の公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉがそれぞれ設けられ、公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉは携帯電話機に固有の秘密復号鍵Ｋｐｎおよびメモリカード固有の秘密復号鍵Ｋｍｃｉによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【００８９】また、データ再生端末（携帯電話機）およびメモリカードのクラス証明書として、ＣｒｔｆｎおよびＣｍｃｉがそれぞれ設けられる。これらのクラス証明書は、メモリカードおよびコンテンツ再生端末のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【００９０】これらのメモリカードおよびコンテンツ再生端末固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａおよび｛ＫＰｐｎ／／Ｃｒｔｆｎ｝ＫＰｍａの形式で、出荷時にメモリカードおよびデータ再生端末（携帯電話機）にそれぞれ記録される。後ほど詳細に説明するが、ＫＰｍａは配信システム全体で共通の公開認証鍵である。

【００９１】図４は、図１に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【００９２】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ３０、携帯電話機１００、メモリカード１１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００９３】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００９４】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００９５】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍと、公開暗号鍵ＫＰｍで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍが存在する。

【００９６】図５は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。

【００９７】ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース

３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベースに保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００９８】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを復号するための公開認証鍵を保持する認証鍵保持部３１３と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰｍａによって復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｉを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００９９】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよび再生期限ＡＣ２を、復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【０１００】ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１０１】図６は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【０１０２】携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのバスＢＳ２と、バスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

【０１０３】携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのキー操作部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データベースＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを含む。

【０１０４】携帯電話機１００は、さらに、音声再生部１１１２の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１１１３と、ＤＡ変換器１１１３の出力を外部出力装置等へ出力するための端子１１１４とを含む。

【０１０５】携帯電話機１００は、さらに、通常の通話動作において、携帯電話機１００のユーザが話した音声信号を入力するマイク１１１５と、マイク１１１５からの音声信号をアナログ信号からディジタル信号に変換するＡＤ変換器１１１６と、ＡＤ変換器１１１６からのディジタル信号を所定の方式に従って符号化してバスＢＳ２へ与える音声符号化部１１１７とを含む。

【０１０６】携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００とを含む。

【０１０７】携帯電話機１００は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｒｔｆ１を公開復号鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを保持する認証データ保持部１２０２を含む。ここで、携帯電話機（データ端末装置）１００のクラスｎは、ｎ＝１であるとする。

【０１０８】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１２０４と、バスＢＳ２から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１２０６とを含む。

【０１０９】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセ

ッションキー発生部１２１０と、発生されたセッションキーＫｓ３を復号処理部１２０６によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ２に出力する暗号化処理部１２０８とを含む。

【０１１０】携帯電話機１００は、さらに、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１２１２とを含む。

【０１１１】携帯電話機１００は、さらに、バスＢＳ２より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１２１２より取得したライセンス鍵Ｋｃによって復号しコンテンツデータを出力する復号処理部１２１４と、復号処理部１２１４の出力を受けてコンテンツデータを再生するための音楽再生部１２１６と、音楽再生部１２１６の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１２１８と、ＤＡ変換器１１１３とＤＡ変換器１２１８との出力を受けて、動作モードに応じて選択的に端子１１１４または端子１２２０から出力するためのスイッチ１２２２と、スイッチ１２２２の出力を受けて、ヘッドホーン１３０と接続するための接続端子１２２４とを含む。

【０１１２】なお、図６においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１１３】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１１４】図７は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃｉおよびＫｍｃｉが設けられ、メモリカードのクラス証明書Ｃｍｃｉが設けられるが、メモリカード１１０においては、これらは自然数ｉ＝１でそれぞれ表わされるものとする。

【０１１５】したがって、メモリカード１１０は、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ１を保持するＫｍｃ１保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Ｋｍ１を保持するＫｍ１保持部１４２１と、Ｋｍ１によって復号可能な公開暗号鍵ＫＰｍ１を保持するＫＰｍ１保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵ＫＰｍｃ１およびクラス証明書Ｃｍｃ１を公開認証鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａとして保持する。

【０１１６】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１１７】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０１を介して授受するインタフェース１４２３と、インタフェース１４２３との間で信号をやり取りするバスＢＳ３と、バスＢＳ３にインタフェース１４２３から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Ｋｍｃ１をＫｍｃ１保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ１を接点Ｐａに出力する復号処理部１４０４と、ＫＰｍａ保持部１４１４から認証鍵ＫＰｍａを受けて、バスＢＳ３に与えられるデータからＫＰｍａによる復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号化処理部１４０６とを含む。

【０１１８】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｎもしくはＫＰｍｃｉによって暗号化してバスＢＳ３に送出する暗号化処理部１４１０と、バスＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号し、復号結果をバスＢＳ４に送出する復号処理部１４１２とを含む。

【０１１９】メモリカード１１０は、さらに、バスＢＳ３上のデータを公開暗号鍵ＫＰｍ１と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号するための復号処理部１４２２と、禁止クラスリストのバージョン更新のためのデータＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬをバスＢＳ４より受けて格納するとともに、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域１４１５Ａと、コンテンツＩＤを含むＨｅａｄｅｒ、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、および暗号化コンテンツデータの関連情報Ｄａｔａ－ｉｎｆを記録したデータ領域１４１５Ｂとから成る。

【０１２０】メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスを保持するため

のライセンス情報保持部１４４０と、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１２１】ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各ライセンスに対応するライセンスをバンクごとに保持する。

【０１２２】なお、図７において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）である。

【０１２３】もちろん、メモリ１４１５も含めて、モジュールＴＲＭ内に組込まれる構成としてもよい。しかしながら、図７に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

【０１２４】以降では、簡単化のためアクセス制御情報ＡＣ１は再生回数の制限を行なう制御情報である再生回数のみを、再生回路制御情報ＡＣ２は再生可能な期限を規定する制御情報である再生期限のみを制限するものとし、アクセス制御情報ＡＣ１および再生回路制御情報ＡＣ２を、それぞれ、再生回数制限ＡＣ１、再生期限ＡＣ２と称するものとする。

【０１２５】図８を参照して、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃと、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２等から成るライセンスとが記録されたメモリカード１１０における各種の状態について説明する。なお、図８においては、再生回数制限ＡＣ１に制限がない場合を「ＦＦ」で表し、再生期限ＡＣ２に制限がない場合を「００」で表している。図８の（ａ）は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンスがメモリカード１１０に記録されており、新たに暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃとライセンスとを配信サーバ３０から受信する場合を示す。また、図８の（ｂ）は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンス鍵Ｋｃが存在し、一部、再生回数制限ＡＣ１によって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの再生が制限されている場合を示す。さらに、図８の（ｃ）は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃとライセンスとが記録されており、一部の暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを再生するライセンスが記録されていない場合を示す。

【０１２６】図８の（ａ）を参照して、コンテンツＩＤ：５５０１９９３０１１２，５５０１９９５１０１３，５５０１９６３０１２２によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）、その暗号化コンテンツデータを復号するためのライセンス鍵：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ，９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５，Ｆ６Ｆ５３６９５１０４ＡＦ３３２３Ｃ３１が記録されている。また、コンテンツＩＤ：５５０１９９５１０１３，５５０１９６３０１２２によって特定される暗号化コンテンツデータは再生回数制限ＡＣ１および再生期限ＡＣ２が無制限であるが、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータは再生回数制限ＡＣ１は２０回、再生期限ＡＣ２は無制限である。したがって、データ領域１４１５Ｂに記録された３つの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃに対するライセンスはライセンス情報保持部１４４０に記録されている。

【０１２７】図８の（ｂ）を参照して、コンテンツＩＤ：５５０１９９３０１１２，５５０１９９５１０１３によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、その暗号化コンテンツデータを復号するためのライセンス鍵：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ，９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５が記録されている。また、コンテンツＩＤ：５５０１９５１０１３によって特定される暗号化コンテンツデータは再生回数制限ＡＣ１および再生期限ＡＣ２が無制限であるが、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータの再生回数制限ＡＣ１は０回、再生期限ＡＣ２は無制限である。したがって、データ領域１４１５Ｂに記録された２つの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのうち、１つの暗号化コンテンツデータはライセンスがライセンス情報保持部１４４０に記録されていない。

【０１２８】図８の（ｃ）を参照して、コンテンツＩＤ：５５０１９９３０１１２，５５０１９９５１０１３によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、その暗号化コンテンツデータを復号するためのライセンス鍵：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ，９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５が記録されている。また、コンテ

ンツＩＤ：５５０１９９５１０１３によって特定される暗号化コンテンツデータは再生回数制限ＡＣ１および再生期限ＡＣ２が無制限であり、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータの再生回数制限ＡＣ１は２０回、再生期限ＡＣ２は無制限である。さらに、コンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）はデータ領域１４１５Ｂに記録されているが、その暗号化コンテンツデータを再生するためのライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２から成るライセンスはライセンス情報保持部１４４０に記録されていない。したがって、データ領域１４１５Ｂに記録された３つの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのうち、１つの暗号化コンテンツデータに対するライセンスが存在しない。

【０１２９】図８を参照して説明したように、メモリカード１１０には、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２が記録されているか否かによって各種の状態が存在する。

【０１３０】次に、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス鍵Ｋｃ等が各種の状態で記録されたメモリカード１１０が携帯電話機１００に装着され、携帯電話機１００のユーザから暗号化コンテンツデータの受信要求がされた場合の動作について説明する。

【０１３１】図９～図１２は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０１３２】図９を参照して、携帯電話機１００のユーザからキー操作部１１０８を介してコンテンツデータの配信要求がなされると、携帯電話機１００は、コンテンツメニューの送信要求を配信サーバ３０へ送信する（ステップＳ７０）。配信サーバ３０の配信制御部３１５は、通信装置３５０およびバスＢＳ１を介してコンテンツメニューの送信要求を受信すると（ステップＳ７２）、メニューデータベース３０７からバスＢＳ１を介してコンテンツメニューを読出し、その読出したコンテンツメニューをバスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ７４）。携帯電話機１１０は、送受信部１１０４によってコンテンツメニューを受信し、コントローラ１１０６は、コンテンツメニューを表示部１１１０に表示する（ステップＳ７６）。

【０１３３】そうすると、携帯電話機１００の表示部１１１０には、図１３に示すコンテンツメニュー６０が表示される。ユーザは、コンテンツメニュー６０の番号００１，００２，００３，・・・を選択することによって配信を希望する暗号化コンテンツデータを選択する。表示部１１１０には、別の画面に移行するための移行部１１１１が設けられている。ユーザは、表示部１１１０に表示されたコンテンツメニュー６０中に希望する暗号化コンテンツデータが表示されていないとき、移行部１１１１をクリックする。移行部１１１１には、別の画面へ移行するためのアドレスが含まれている。

【０１３４】携帯電話機１００のコントローラ１１０６は、コンテンツが選択された否かを判断し（ステップＳ７８）、移行部１１１１がクリックされると、コントローラ１１０６は、移行部１１１１に含まれるアドレスを送受信部１１０４を介して配信サーバ３０へ送信し、別の画面を送信するように要求する。そして、ステップＳ７０～Ｓ７８が繰返される。つまり、コンテンツメニューは、コンテンツメニュー６０から成る複数個の画面が階層的に配列されて構成されており、各画面は、ジャンルの異なる暗号化コンテンツデータ、同じジャンルであるが、他の暗号化コンテンツデータ等から成るコンテンツメニューによって構成されている。

【０１３５】そして、配信サーバ３０から複数の画面によって送られてきたコンテンツメニューに、希望する暗号化コンテンツデータが含まれていないとき、配信動作はステップＳ１７０へ移行し、配信動作は終了する。

【０１３６】コンテンツメニュー６０は、暗号化コンテンツデータを特定するためのコンテンツＩＤを含んでおり、ステップＳ７８において暗号化コンテンツデータが選択されたとき、コンテンツメニューから選択された暗号化コンテンツデータのコンテンツＩＤが抽出される（ステップＳ８０）。

【０１３７】そして、キー操作部１１０８を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ８２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータの再生回数制限ＡＣ１、および再生期限ＡＣ２を設定して購入条件ＡＣが入力される。

【０１３８】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１０６は、選択された暗号化コンテンツデータに対するコンテンツＩＤと同じコンテンツＩＤを有する暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されていないかを検索する（ステップＳ８４）。この場合、コントローラ１１０６は、選択された暗号化コンテンツデータに対応するコンテンツＩＤをメモリインタフェース１２００を介してメモリカード１１０へ送信する。メモリカード１１０のコントローラ１４２０は、インタフェース１４２３およびバスＢＳ３を介して携帯電話機１００からコンテンツＩＤを受取り、その受取ったコンテンツＩＤがメモリ１４１５のＨｅａｄｅｒ１４２４に含まれるコンテンツＩＤと一致するか否かによって、ユーザがコンテン

ツメニューから選択した暗号化コンテンツデータがメモリカード１１０に記録されているか否かを検索する。

【０１３９】この場合、メモリカード１１０のメモリ１４１５に記録されたＨｅａｄｅｒ、Ｄａｔａ－ｉｎｆ、および｛Ｄａｔａ｝Ｋｃを図１４に示すように１つのデータ列としてハッシュ関数などを用いた署名データを併せて取扱うようにすれば、コンテンツＩＤの改組を防止することができる。署名の確認は、コンテンツＩＤの検査時に対応したものに関しても行なえば良い。

【０１４０】そして、コントローラ１１０６は、選択した暗号化コンテンツデータがメモリカード１１０に記録されているか否かを判断し（ステップＳ８６）、暗号化コンテンツデータがメモリカード１１０に記録されていないとき、データを配信サーバ３０から取得するためのフラグ”Ｙｅｓ”を立てる（ステップＳ８８）。暗号化コンテンツデータがメモリカード１１０に記録されているとき、ライセンスの確認が行なわれる（ステップＳ９０）。つまり、図８を参照して説明したようにライセンス鍵ＫｃがメモリカードＫ１１０に記録されているか、再生回数制限ＡＣ１および再生期限ＡＣ２によって暗号化コンテンツデータの再生が制限されていないかによってライセンスの確認が行なわれる。ライセンスが存在しないときはステップＳ９４へ移行する。ライセンスが存在し、暗号化コンテンツデータが再生できる場合、コントローラ１１０６は、「ライセンス単体購入？」を表示部１１１０に表示し、ライセンスだけを単体で購入するか否かの意思を確信する（ステップＳ９２）。コントローラ１１０６は、ライセンスだけを購入しない旨の指示がキー操作部１１０８から入力されると、ステップＳ１７０へ移行し、暗号化コンテンツデータの配信動作は終了する。コントローラ１１０６は、ライセンスだけを単体で購入する旨の指示がキー操作部１１０８から入力されると、データを配信サーバ３０から取得しないフラグ”Ｎｏ”を立てる（ステップＳ９４）。

【０１４１】次に、図１０を参照して、携帯電話機１００は、ユーザが暗号化コンテンツデータを選択することによって抽出したコンテンツＩＤ（ステップＳ８０参照）の指定による配信リクエストがなされる（ステップＳ１００）。

【０１４２】メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａが出力される（ステップＳ１０２）。

【０１４３】携帯電話機１００は、メモリカード１１０からの認証のための認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

【０１４４】配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａ、ライセンス購入条件のデータＡＣを受信し（ステップＳ１０６）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰｍａで復号処理を実行する（ステップＳ１０８）。

【０１４５】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍｃ１と証明書Ｃｍｃ１を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１０）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を承認し、受理する。そして、次の処理（ステップＳ１１２）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を受理しないで処理を終了する（ステップＳ１７０）。

【０１４６】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍｃ１が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

【０１４７】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

【０１４８】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１３）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ１によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

【０１４９】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍｃ１として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

【０１５０】携帯電話機１００が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍｃ１を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、バスＢＳ３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に

保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ１により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１２０）。

【０１５１】コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生器１４１８に対して、メモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

【０１５２】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストのデータＣＲＬ＿ｄａｔａをメモリ１４１５から抽出してバスＢＳ４に出力する。

【０１５３】暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍ１および禁止クラスリストのデータＣＲＬ＿ｄａｔａを１つのデータ列として暗号化して、｛Ｋｓ２//ＫＰｍ１//ＣＲＬ＿ｄａｔ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１２２）。

【０１５４】バスＢＳ３に出力された暗号化データ｛Ｋｓ２//ＫＰｍ１//ＣＲＬ＿ｖｅｒ｝Ｋｓ１は、バスＢＳ３からインタフェース１４２３、端子１２０１およびメモリインタフェース１２００を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

【０１５５】配信サーバ３０は、トランザクションＩＤ//｛Ｋｓ２//ＫＰｍ１//ＣＲＬ＿ｄａｔ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍ１およびメモリカード１１０における禁止クラスリストのデータＣＲＬ＿ｄａｔａを受理する（ステップＳ１２６）。

【０１５６】配信制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、ライセンスＩＤ、アクセス制限情報ＡＣ１および再生期限ＡＣ２を生成する（ステップＳ１２８）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１３０）。

【０１５７】配信制御部３１５は、生成したライセンス、すなわち、ライセンス鍵Ｋｃ、再生期限ＡＣ２、ライセンスＩＤ、コンテンツＩＤ、およびアクセス制限情報ＡＣ１を暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ１によってライセンスを暗号化する（ステップＳ１３２）図１１を参照して、配信サーバ３０において、メモリカード１１０から送信された禁止クラスリストのデータＣＲＬ＿ｄａｔが最新か否かが判断され、データＣＲＬ＿ｄａｔが最新と判断されたとき、ステップＳ１３４へ移行する。また、データＣＲＬ＿ｄａｔが最新でないときはステップＳ１３７へ移行する（ステップＳ１３３）。

【０１５８】データＣＲＬ＿ｄａｔが最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛Ｋｃ//ＡＣ２//ライセンスＩＤ//コンテンツＩＤ//ＡＣ１｝Ｋｍ１をメモリカード１１０において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛Ｋｃ//ＡＣ２//ライセンスＩＤ//コンテンツＩＤ//ＡＣ１｝Ｋｍ１｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛Ｋｃ//ＡＣ２//ライセンスＩＤ//コンテンツＩＤ//ＡＣ１｝Ｋｍ１｝Ｋｓ２を通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ１３４）。

【０１５９】そして、携帯電話機１００は、暗号化データ｛Ｋｃ//ＡＣ２//ライセンスＩＤ//コンテンツＩＤ//ＡＣ１｝Ｋｍ１｝Ｋｓ２を受信し（ステップＳ１３５）、バスＢＳ２およびメモリインタフェース１２００を介してメモリカード１１０へ送信する。メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛Ｋｃ//ＡＣ２//ライセンスＩＤ//コンテンツＩＤ//ＡＣ１｝Ｋｍ１｝Ｋｓ２を端子１２０１およびインタフェース１４２３を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛Ｋｃ//ＡＣ２//ライセンスＩＤ//コンテンツＩＤ//ＡＣ１｝Ｋｍ１を受理する（ステップＳ１３６）。その後、ステップＳ１４６へ移行する。

【０１６０】一方、配信サーバ３０において、ＣＲＬ＿ｄａｔが最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストのデータＣＲＬ＿ｄａｔを取得する（ステップＳ１３７）。

【０１６１】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの最新データＣＲＬ＿ｄａｔとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、バスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

【０１６２】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行な

うことができ、データ配信システムのセキュリティを向上させることができる。

【0163】携帯電話機100は、送信された暗号化データ｛｛Kc//AC2//ライセンスID//コンテンツID//AC1｝Km1//CRL_dat｝Ks2を受信し（ステップS140）、メモリインタフェース1200を介してメモリカード110へ出力する。メモリカード110においては、端子1201およびインタフェース1423を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3の受信データを復号しバスBS4に出力する（ステップS142）。

【0164】この段階で、バスBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス｛Kc//AC2//ライセンスID//コンテンツID//AC1｝Km1と、CRL_datとが出力される（ステップS142）。コントローラ1420の指示によって受理した最新の禁止クラスリストCRL_datによってメモリ1415内の禁止クラスリストCRLが書き換えられる（ステップS144）。

【0165】ステップS134，S135，S136は、メモリカード110から送られてきた禁止クラスリストCRL_datが最新の場合のライセンス鍵Kc等のメモリカード110への配信動作であり、ステップS137，S138，S140，S142，S144は、メモリカード110から送られてきた禁止クラスリストCRL_datが最新でない場合のライセンス鍵Kc等のメモリカード110への配信動作である。このように、メモリカード110から送られてきた禁止クラスリストCRL_datが更新されているか否かを、逐一、確認し、更新されていないとき、最新の禁止クラスリストCRL_datをCRLデータベース306から取得し、メモリカード110に配信することによって、ライセンスの破られたメモリカードへの暗号化コンテンツデータ｛Data｝Kcの配信を防止し、かつ、ライセンスの破られた携帯電話機による暗号化コンテンツデータ｛Data｝Kcの再生を防止できる。

【0166】ステップS136またはステップS144の後、コントローラ1420の指示によって、暗号化ライセンス｛Kc//AC2//ライセンスID//コンテンツID//AC1｝Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンス（ライセンス鍵Kc、ライセンスID、コンテンツID、再生回数制限AC1および再生期限AC2）が受理される（ステップS148）。

【0167】コントローラ1420は、ライセンスをライセンス情報保持部1440に記録する（ステップS150）。

【0168】図12を参照して、携帯電話機100のコントローラ1106は、ステップS88およびステップS94において立てたフラグを参照し、配信サーバ30から暗号化コンテンツデータを取得するか否かを判断する。そして、暗号化コンテンツデータを配信サーバ30から取得しないとき、ステップS164へ移行し、暗号化コンテンツデータを配信サーバ30から取得するとき、ステップS154へ移行する。

【0169】暗号化コンテンツデータを配信サーバ30から取得するとき、携帯電話機100は、配信サーバ30から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ30へ送信する（ステップ154）。

【0170】配信サーバ30は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し（ステップS156）、情報データベース304より、暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data-infを取得して、これらのデータをバスBS1および通信装置350を介して出力する（ステップS158）。

【0171】携帯電話機100は、｛Data｝Kc//Data-infを受信して、暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data-infを受理する（ステップS160）。暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data-infは、メモリインタフェース1200、端子1201、およびインタフェース1423を介してメモリカード110のバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ｛Data｝Kcおよび付加情報Data-infがそのままメモリ1415に記録される（ステップS162）。

【0172】そして、ステップS152において暗号化コンテンツデータを配信サーバ30から受信しないと判断されたときも含め、メモリカード110から配信サーバ30へは、トランザクションID//配信受理の通知が送信され（ステップS164）、配信サーバ30でトランザクションID//配信受理を受信すると（ステップS166）、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行われて配信終了の処理が実行され（ステップS168）、全体の処理が終了する（ステップS170）。

【0173】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信できた公開暗号鍵Kp1およびKmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kp1およびKmc1による暗号化が破られたクラス証明書リストに記

載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0174】また、配信サーバ30への暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求時にメモリカード110における暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、ライセンス鍵Ｋｃ、および再生回数制限ＡＣ１等の記録状況に応じて、必要な配信だけを配信サーバ30に要求することができる。その結果、無駄な配信を防止することができる。

【0175】次に、図15および図16を参照してメモリカード110に配信されたコンテンツデータの携帯電話機100における再生動作について説明する。図15を参照して、再生動作の開始とともに、携帯電話機100のユーザからキー操作部1108を介して再生指示が携帯電話機100にインプットされる（ステップＳ200）。そうすると、コントローラ1106は、バスＢＳ2を介して認証データ保持部1202から認証データ｛ＫＰｐ1／／Ｃｒｔｆ1｝ＫＰｍａを読出し、メモリインタフェース1200を介してメモリカード110へ認証データ｛ＫＰｐ1／／Ｃｒｔｆ1｝ＫＰｍａを入力する（ステップＳ201）。

【0176】そうすると、メモリカード110は、認証データ（ＫＰｐ1／／Ｃｒｔｆ1｝ＫＰｍａを受理する（ステップＳ202）。そして、メモリカード110の復号処理部1408は、受理した認証データ｛ＫＰｐ1／／Ｃｒｔｆ1｝ＫＰｍａを、ＫＰｍａ保持部1414に保持された公開認証鍵ＫＰｍａによって復号し（ステップＳ203）、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ1／／Ｃｒｔｆ1｝ＫＰｍａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ204）。復号できなかった場合、コントローラ1420は認証データ不受理の出力をデータＢＳ3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する（ステップＳ206）。認証データが復号できた場合、コントローラ1420は、取得した証明書Ｃｒｔｆ1がメモリ1415から読出した禁止クラスリストデータに含まれるか否かを判断する（ステップＳ205）。この場合、証明書Ｃｒｔｆ1にはＩＤが付与されており、コントローラ1420は、受理した証明書Ｃｒｔｆ1のＩＤが禁止クラスリストデータの中に存在するか否かを判別する。証明書Ｃｒｔｆ1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータＢＳ3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する（ステップＳ206）。

【0177】ステップＳ204において認証データが公開認証鍵ＫＰｍａで復号できなかったとき、およびステップＳ205において受理した証明書Ｃｒｔｆ1が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ1110に表示する（ステップＳ207）。

【0178】ステップＳ205において、証明書Ｃｒｔｆ1が禁止クラスリストデータに含まれていないと判断されると、図16を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーＫｓ2を発生させる（ステップＳ208）。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーＫｓ2を、復号処理部1408で復号された公開暗号鍵ＫＰｐ1によって暗号化した｛Ｋｓ2｝Ｋｐ1をバスＢＳ3へ出力する（ステップＳ209）。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ｛Ｋｓ2｝Ｋｐ1を出力し、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して｛Ｋｓ2｝Ｋｐ1を取得する。そして、Ｋｐ1保持部1204は、秘密復号鍵Ｋｐ1を復号処理部1206へ出力する。

【0179】復号処理部1206は、Ｋｐ1保持部1204から出力された、公開暗号鍵ＫＰｐ1と対になっている秘密復号鍵Ｋｐ1によって｛Ｋｓ2｝Ｋｐ1を復号し、セッションキーＫｓ2を暗号処理部1208へ出力する（ステップＳ210）。そうすると、セッションキー発生部1210は、再生セッション用のセッションキーＫｓ3を発生させ、セッションキーＫｓ3を暗号処理部1208へ出力する（ステップＳ211）。暗号処理部1208は、セッションキー発生部1210からのセッションキーＫｓ3を復号処理部1206からのセッションキーＫｓ2によって暗号化して｛Ｋｓ3｝Ｋｓ2を出力し、コントローラ1106は、バスＢＳ2およびメモリインタフェース1200を介して｛Ｋｓ3｝Ｋｓ2をメモリカード110へ出力する（ステップＳ212）。

【0180】メモリカード110の復号処理部1412は、端子1201、インタフェース1423、およびバスＢＳ3を介して｛Ｋｓ3｝Ｋｓ2を入力し、セッションキー発生部1418によって発生されたセッションキーＫｓ2によって｛Ｋｓ3｝Ｋｓ2を復号して、携帯電話機100で発生されたセッションキーＫｓ3を取得する（ステップＳ213）。

【0181】セッションキーＫｓ3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報ＡＣ1を確認する（ステップＳ214）。

【０１８２】ステップＳ２１４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数制限に制限がある場合にはアクセス制限情報ＡＣ１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ２１５）。一方、アクセス制限情報ＡＣ１によって再生回数制限が制限されていない場合においては、ステップＳ２１５はスキップされ、再生回数制限ＡＣ１は更新されることなく処理が次のステップ（ステップＳ２１６）に進行される。

【０１８３】また、ライセンス情報保持部１４４０内にリクエスト曲の当該コンテンツＩＤが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【０１８４】ステップＳ２１４において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部１４４０に記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生期限ＡＣ２がバスＢＳ４上に出力される（ステップＳ２１６）。

【０１８５】得られたライセンス鍵Ｋｃと再生期限ＡＣ２は、切換スイッチ１４４４の接点Ｐｄを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｄを介して復号処理部１４１２より受けたセッションキーＫｓ３によってバスＢＳ４から受けたライセンス鍵Ｋｃと再生期限ＡＣ２とを暗号化し、｛Ｋｃ／／ＡＣ２｝Ｋｓ３をバスＢＳ３に出力する（ステップＳ２１７）。

【０１８６】バスＢＳ３に出力された暗号化データは、インタフェース１４２３、端子１２０２、およびメモリインタフェース１２００を介して携帯電話機１００に送出される。

【０１８７】携帯電話機１００においては、メモリインタフェース１２００を介してバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｓ３を復号処理部１２１２によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生期限ＡＣ２を受理する（ステップＳ２１８）。復号処理部１２１２は、ライセンス鍵Ｋｃを復号処理部１２１４に伝達し、再生期限ＡＣ２をバスＢＳ２に出力する。

【０１８８】コントローラ１１０６は、バスＢＳ２を介して、再生期限ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２１９）。

【０１８９】ステップＳ２１９においては、再生期限ＡＣ２によって再生不可と判断される場合には、再生動作は終了される。

【０１９０】ステップＳ２１９において再生可能と判断された場合、コントローラ１１０６は、メモリインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ３および端子１２０１を介してメモリインタフェース１２００へ出力する（ステップＳ２２０）。

【０１９１】携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１４へ与える。そして、復号処理部１２１４は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１２から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ２２１）。

【０１９２】そして、復号されたコンテンツデータＤａｔａは音楽再生部１２１６へ出力され、音楽再生部１２１６は、コンテンツデータを再生し、ＤＡ変換器１２１Ｓはディジタル信号をアナログ信号に変換して端子１２２０へ出力する。そして、スイッチ１２２２は端子１２２０を選択して音楽データは端子１２２４を介してヘッドホーン１３０へ出力されて再生される（ステップＳ２２２）。これによって再生動作が終了する。

【０１９３】図１７を参照して、メモリカード１１０における暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス鍵Ｋｃ等の記録状況に応じた暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンス鍵Ｋｃ等の配信の例について説明する。図１７の（ａ）を参照して、メモリカード１１０のデータ領域１４１５Ｂには、暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）と、それぞれの関連情報Ｄａｔａ－ｉｎｆｏとが記録されている。また、ライセンス領域１４１５Ａには、コンテンツＩＤ：５５０１９９３０１１２、トランザクションＩＤ：０００００００００１、ライセンス鍵Ｋｃ：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ、再生回数制限ＡＣ１：００、再生期限ＡＣ２：００のライセンスＬＳ１と、コンテンツＩＤ：５５０１９９５１０１３、トランザクションＩＤ：０００００００３００５、ライセンス鍵Ｋｃ：９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５、再生回数制限ＡＣ１：ＦＦ、再生期限ＡＣ２：００のライセンスＬＳ２とが記録されている。そして、ライセンスＬＳ１については、再生回数制限ＡＣ１は「００」であるので、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）を再生できない、すなわち、ライセンスがない状態を示している。また、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２

２）について、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２が記録されておらず、ライセンスがない状態を示している。つまり、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）に対するライセンスＬＳ２だけが存在し、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、および｛Ｄａｔａ（５５０１９６３０１２２｝Ｋｃ（５５０１９６３０１２２）に対するライセンスが存在しない状況である。

【０１９４】図１７の（ａ）に示すメモリカード１１０の状況において、携帯電話機１００のユーザからコンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求がキー操作部１１０８を介して入力されると、図９のステップＳ７０～Ｓ７８が行なわれ、コンテンツＩＤ：５５０１９９３０１１２が抽出される（ステップＳ８０）。そして、ステップＳ８２において、「２０」回まで再生可能とするライセンスの購入条件ＡＣが入力される。そして、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されているか否かが検索される（ステップＳ８４）。

【０１９５】この場合、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、メモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）として記録されているので、図９のステップＳ８６を介してステップＳ９０へ移行する。そして、ステップＳ９０において、ライセンスによって暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）が再生可能か否かが判断される。この場合、再生回数制限ＡＣ１が「００」であるので、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）を再生することができない。したがって、ステップＳ９０からステップＳ９４へ移行する。そして、ステップＳ９４においてデータ取得＝”Ｎｏ”のフラグが立てられ後、ステップＳ１００～ステップＳ１７０によって再生回数制限ＡＣ１を「２０」回とするライセンスだけが配信サーバ３０からメモリカード１１０に配信される。そして、図１７の（ｂ）に示すようにライセンスＬＳ１の再生回数制限ＡＣ１が「２０」と変更される。これによって、ライセンスＬＳ１によって暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）を再生することができる。

【０１９６】また、図１７の（ａ）に示すメモリカード１１０の状況において、携帯電話機１００のユーザからコンテンツＩＤ：５５０１２３４５６７８によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求がキー操作部１１０８を介して入力されると、図９のステップＳ７０～Ｓ７８が行なわれ、コンテンツＩＤ：５５０１２３４５６７８が抽出される（ステップＳ８０）。その後、ライセンスの購入条件ＡＣとして、ＡＣ１：ＦＦ、ＡＣ２：００の再生制限なしが入力される（ステップＳ８２）。そして、コンテンツＩＤ：５５０１２３４５６７８によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されているか否かが検索される（ステップＳ８４）。この場合、コンテンツＩＤ：５５０１２３４５６７８によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃはメモリカード１１０に記録されていないので、ステップＳ８６からステップＳ８８へ移行し、ステップＳ８８においてデータ取得＝”Ｙｅｓ”のフラグが立てられる。

【０１９７】その後、ステップＳ１００～ステップＳ１７０が実行され、メモリカード１１０にコンテンツＩＤ：５５０１２３４５６７８、トランザクションＩＤ：０００００５５００３４５、ライセンス鍵Ｋｃ：Ｃ６Ｆ５６９５１０４５６ＡＢ３３Ｃ４、再生回数制限ＡＣ１：ＦＦ、再生期限ＡＣ２：００、暗号化コンテンツデータ：｛Ｄａｔａ（５５０１２３４５６７８）｝Ｋｃ（５５０１２３４５６７８）、および関連情報ＤａｔａＤ－ｉｎｆ（５５０１２３４５６７８）が配信され、かつ、記録される。これによって、メモリカード１１０は、図１７の（ｃ）に示す状態になり、ユーザが配信要求を行なった暗号化コンテンツデータ｛Ｄａｔａ（５５０１２３４５６７８）｝Ｋｃ（５５０１２３４５６７８）の再生が可能となる。

【０１９８】さらに、図１７の（ａ）に示すメモリカード１１０の状況において、携帯電話機１００のユーザからコンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求がキー操作部１１０８を介して入力されると、図９のステップＳ７０～Ｓ７８が行なわれ、コンテンツＩＤ：５５０１９６３０１２２が抽出される（ステップＳ８０）。その後、ライセンスの購入条件ＡＣとして、ＡＣ１：ＦＦ、ＡＣ２：００の再生制限なしが入力される（ステップＳ８２）。そして、コンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されているか否かが検索される（ステップＳ８４）。この場合、コンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃはメモリカード１１０に記録されているので、ステップＳ８６からステップＳ９０へ移行する。そして、ステップＳ９０において、ライセンスによって暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）が再生可能か否かが判断さ

れる。この場合、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣのいずれもメモリカード１１０に記録されていないので、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）を再生することができない。したがって、ステップＳ９０からステップＳ９４へ移行する。

【０１９９】そして、ステップＳ９４においてデータ取得＝”Ｎｏ”のフラグが立てられた後、ステップＳ１００～ステップＳ１７０によって再生制限なしとするライセンスだけが配信サーバ３０からメモリカード１１０に配信される。そして、図１７の（ｄ）に示すようにコンテンツＩＤ：５５０１９６３０１２２、トランザクションＩＤ：０００００５５０３３９、ライセンス鍵Ｋｃ：Ｆ６Ｆ５３６９５１０４ＡＦ３３２３Ｃ３１、再生回数制限ＡＣ１：ＦＦ、および再生期限：００がメモリカード１１０のライセンス領域１４１５Ａに記録される。これによって、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）を再生することができる。

【０２００】上述したように、携帯電話機１００のユーザは、メモリカード１１０における暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス鍵Ｋｃ等の記録状況に応じて、携帯電話機１００を用いて配信サーバ３０から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンス鍵Ｋｃ等をメモリカード１１０に受信し、ライセンス鍵Ｋｃによって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号し、かつ、再生することができる。

【０２０１】上記においては、携帯電話機１００のユーザが暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求を行なうとき、メモリカード１１０に記録されている暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、配信サーバ３０から受信した暗号化コンテンツデータであるとして説明したが、本発明においては、かかる場合に限らず、配信サーバ３０以外から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃだけを受信し、メモリカード１１０に記録した場合も含まれる。

【０２０２】図１８および図１９を参照して、配信サーバ３０以外の装置から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受信し、その暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをメモリカード１１０に記録する場合について説明する。

【０２０３】図１８を参照して、コンピュータ１４０を用いた暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信について説明する。携帯電話機１００にはメモリカード１１０が着脱可能であり、音楽を再生するためのヘッドホン１３０が接続されている。そして、携帯電話機１００は、通信ケーブル１４５を介してコンピュータ１４０と接続されている。

【０２０４】コンピュータ１４０は、ハードディスク１４１と、コントローラ１４２と、外部インタフェース１４３とを備える。そして、ハードディスク１４１はバスＢＳ５を介してコントローラ１４２と接続され、コントローラ１４２はライセンス保護モジュール１４３を含む。

【０２０５】ハードディスク１４１は、インターネット配信によってコンピュータ１４０に配信された暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをバスバス５を介して記憶する。コントローラ１４２は、携帯電話機１００のユーザから通信ケーブル１４５および外部インタフェース１４３を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの送信要求があると、ハードディスク１４１から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを読出し、外部インタフェース１４３を介して外部へ出力する。

【０２０６】外部インタフェース１４３は、携帯電話機１００から通信ケーブル１４５を介してコンピュータ１４０に入力された信号をコントローラ１４２に入力するとともに、コントローラ１４２からの信号を外部へ出力する。

【０２０７】ライセンス保護モジュール１４４は、図５に示すデータ処理部３１０と同じ構成を有し、携帯電話機１００に装着されたメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを送信するために、上述したように携帯電話機１００およびメモリカード１１０と公開暗号鍵、セッションキー等のやり取りを行ないながら、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを保護してメモリカード１１０へ送信するものである。

【０２０８】インターネット配信によって配信サーバからコンピュータ１４０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃが配信され、コンピュータ１４０のハードディスク１４１にバスＢＳ５を介して暗号化コンテンツデータが記憶されている。

【０２０９】携帯電話機１００のユーザがキー操作部１０８から送信要求を入力すると、通信ケーブル１４５および外部インタフェース１４３を介して送信要求がコントローラ１４２に入力される。コントローラ１４２は、送信要求を受付けると、要求された暗号化コンテンツデータ｛Ｄａｔａ｝ＫｃをバスＢＳ５を介してハードディスク１４１から読出し、ライセンス保護モジュール１４４に入力する。

【０２１０】ライセンス保護モジュール１４４は、上述したようにメモリカード１１０と通信ケーブル１４５を介して公開暗号鍵、セッションキー等のやり取りを行ない、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをメモリカード１１０へ送信する。

【０２１１】送信後、携帯電話機１００のユーザは、上述したのと同じ方法によって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのライセンス（コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２）を配信サーバ３０から配信してもらい、暗号化コ

ンテンツデータ｛Ｄａｔａ｝Ｋｃを再生する。

【０２１２】ＣＤを用いた場合、音楽ＣＤから取得して生成した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、一旦、ハードディスク１４１に記録してからメモリカード１１０へ送信しても良いし、ハードディスク１４１に送信せずに、直接、メモリカード１１０へ送信しても良い。

【０２１３】暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、図１９に示すようにメモリカード１１０を、直接、コンピュータ１４０に装着してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを記録しても良い。この場合、コンピュータ１４０のコントローラ１４２は、ライセンス保護モジュール１４４によって、直接、メモリカード１１０に暗号化コンテンツデータを記録する。

【０２１４】図１９においても、コンピュータ１４０は、図１８に示す場合と同じ方法により暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得する。

【０２１５】携帯電話機１００が、新たに受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃに対応するライセンス鍵を含むライセンスの配信要求を配信サーバ３０へ行なう場合のフローチャート、および新たに受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを再生するフローチャートは、図９～図１２、および図１５，１６に示すフローチャートと同じである。

【０２１６】再生回数期限ＡＣ１および再生期限ＡＣ２を、それぞれ、再生回数制限と再生期限として説明したが、再生回数期限ＡＣ１は記録装置でのライセンスの扱いに制限を加える制御情報であればよく、また、再生回数はデータ再生端末における再生に対して制限を加えるものであれば何れの制限を行ってもかまわない。

【０２１７】また、携帯電話機１００を暗号化コンテンツデータまたはライセンスの配信を受けるデータ端末装置として説明したが、特に通話機能等は必要なく、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【０２１８】さらには、携帯電話機１００はコンテンツデータ（音楽データ）を再生する機能を備えているが、必ずしもデータ再生機能を必要とせず、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【０２１９】またさらに、着脱可能な記録装置であるメモリカードに暗号化コンテンツデータまたはライセンスを記録するように説明したが、メモリカードに限定するものではない。そして、実施の形態においては、着脱可能な記録装置である必要もない。

【０２２０】本発明の実施の形態によれば、携帯電話機は、ユーザから暗号化コンテンツデータの配信要求が入力されると、装着されたメモリカードの記録状況を検索し、その記録状況に応じて必要な暗号化コンテンツデータ、およびライセンス鍵等だけを配信サーバから受信するので、暗号化コンテンツデータ、およびライセンス鍵等が重複してメモリカードに記録されることがない。また、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。さらに、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【０２２１】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

【図５】　ライセンスサーバの構成を示す概略ブロック図である。

【図６】　携帯電話機の構成を示すブロック図である。

【図７】　メモリカードの構成を示すブロック図である。

【図８】　メモリカードの記録状態を説明するための概念図である。

【図９】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図１０】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１１】　図１に示すデータ配信システムにおける配信動作を説明するための第３のフローチャートである。

【図１２】　図１に示すデータ配信システムにおける配信動作を説明するための第４のフローチャートである。

【図１３】　配信サーバから携帯電話機に送信されたコンテンツメニューを携帯電話機の表示部に表示した状態を示す図である。

【図１４】　メモリカードのメモリにおけるデータフォーマットである。

【図１５】　携帯電話機における再生動作を説明するための第１のフローチャートである。

【図１６】　携帯電話機における再生動作を説明するための第２のフローチャートである。

【図１７】　メモリカードの記録状況に応じた暗号化コンテンツデータおよびライセンスの配信例を説明する図

である。

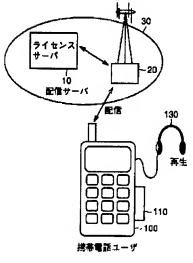
【図18】 コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための概略図である。

【図19】 コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための他の概略図である。

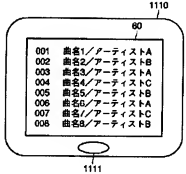
【符号の説明】

10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、60 コンテンツメニュー、100 携帯電話機、110 メモリカード、130 ヘッドホン、140 コンピュータ、141 ハードディスク、142，1106，1420 コントローラ、143 外部インタフェース、144 ライセンス保 護モジュール、145 通信ケーブル、302 課金データベース、304情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312，320，1206，1212，1214，1404，1408，1412，1422復号処理部、313 認証鍵保持部、315 配信制御部、316，1210，1418 セッションキー発生部、318，326，328，1208，1406，1410 暗号処理部、350 通信装置、1102 アンテナ、1104送受信部、1108 キー操作部、1110 ディスプレイ、1111 移行部、1112 音声再生部、1113，1218 DA変換器、1114，1201，1220，1224 端子、1115 マイク、1116 AD変換器、1117 音声符号化部、1200 メモリインタフェース、1202，1400 認証データ保持部、1204 Kp1保持部、1216 音楽再生部、1222 スイッチ、1402 Kmc1保持部、1414 KPma保持部、1415 メモリ、1415A CRL領域、1415B データ領域、1416KPm1保持部、1421 Km1保持部、1423 インタフェース、1424 Header、1440 ライセンス情報保持部、1442，1444，1446 切換スイッチ。

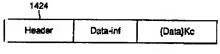
【図1】



【図13】



【図14】



【図4】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵（非対称鍵）	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

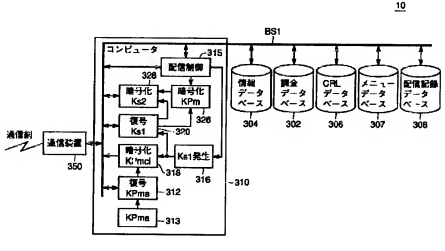
【図2】

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ、アップデートプログラム
Kc	ライセンス鍵		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文形態
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可）
トランザクションID	ライセンス固有		記信を特定するための管理コード
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(記録再生機構)における制御情報(例：再生可否)

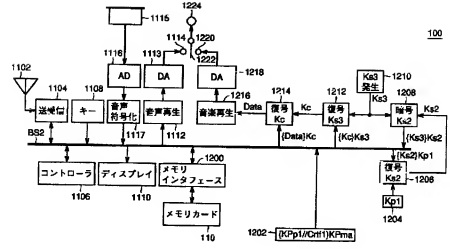
【図3】

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵（非対称鍵）	携帯電話機	Kpnにて復号可能。 {KPpn/Crtn}KPmaの形式で出荷時に記録 ＊携帯電話機の種類ごとに異なる。
KPmcl	公開暗号鍵（非対称鍵）	メモリカード	Kmclにて復号可能。 {KPmcl/Cmcl}KPmaの形式で出荷時に記録 ＊メモリカードの種類ごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の記号鍵 ＊携帯電話機の種類ごとに異なる。
Kmcl	秘密復号鍵	メモリカード	メモリカード固有の記号鍵 ＊メモリカードの種類ごとに異なる。
Crtn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。鍵証機能を有する。 {KPpn/Crtn}KPmaの形式で出荷時に記録 ＊携帯電話機のクラスごとに異なる。
Cmcl		メモリカード	メモリカードのクラス証明書。鍵証機能を有する。 {KPmcl/Cmcl}KPmaの形式で出荷時に記録 ＊メモリカードのクラスごとに異なる。

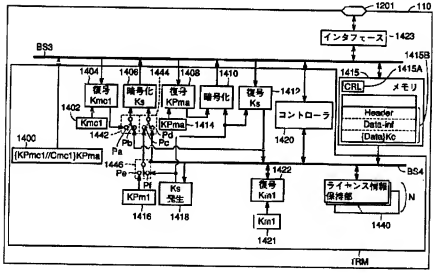
【図5】



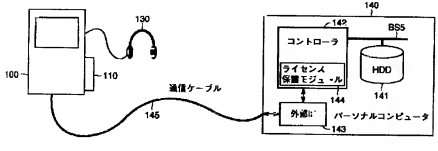
【図6】


1224
1115
1114
1220
1222
100
1116
1113
1102
AD
DA
DA
1218
Ka3
発生
1210
1104
1108
1216
1214
1212
1208
Ka3
送受信
キー
音声
符号化
音声再生
音楽再生
Data
復号
Kc
Kc
復号
Ks3
暗号
Ks2
Ks2
BS2
1117
1112
{Data}Kc
{Kc}Ks3
{Ks3}Ks2
{Ks2}Kp1
1200
復号
Ks2
1206
コントローラ
ディスプレイ
メモリ
インタフェース
Kp1
1106
1110
1204
メモリカード
110
1202
{KPp1//Cnt1}KPma

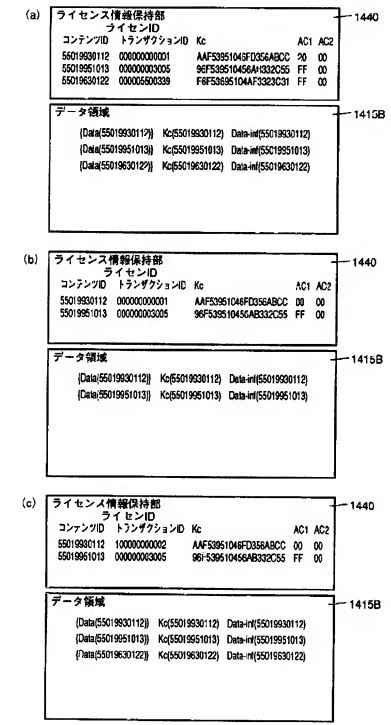
【図7】


1201
110
インタフェース
1423
BS3
1415B
1415A
1404
1406
1444
1408
1410
1415
メモリ
CRL
復号
Kmc1
暗号化
Ks
復号
KPma
暗号化
復号
Ks
1412
Header
Data-inf
{Data}Kc
1402
Kmc1
KPma
1414
コントローラ
1442
Pd
Pc
1420
1400
Pb
Pa
{KPmc1//Cmc1}KPma
1446
Pe
1422
BS4
Pf
KPm1
Ks
発生
復号
Kin1
ライセンス情報
保持部
N
1416
1418
Kin1
1440
1421
tRM

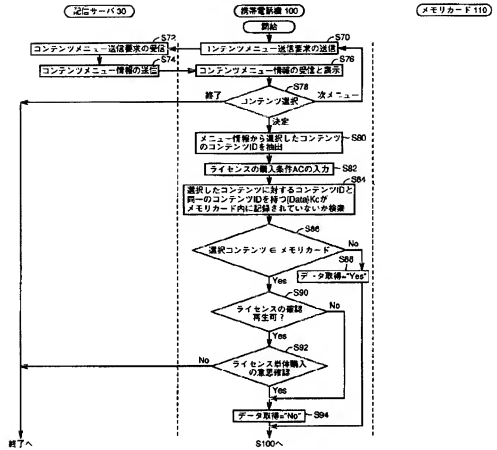
【図18】


130
140
142
BS5
コントローラ
100
110
ライセンス
保管モジュール
HDD
通信ケーブル
144
141
145
外部I/F
パーソナルコンピュータ
143

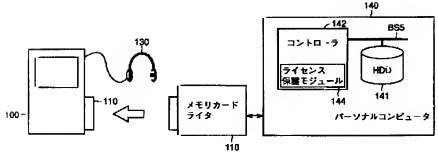
【図8】


(a)
ライセンス情報保持部
ライセンスID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 000000000001 AAF53951046FD356ABCC 00 00
55019951013 000000003005 96F53951045AAB332C55 FF 00
55019630122 090005600339 F6F53695104AF3323C31 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B
(b)
ライセンス情報保持部
ライセンスID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 000000000001 AAF53951046FD356ABCC 00 00
55019951013 000000003005 96F53951045AAB332C55 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
1415B
(c)
ライセンス情報保持部
ライセンスID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 100000000002 AAF53951046FD356ABCC 00 00
55019961013 000000003005 96i-539510456AB332C55 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B

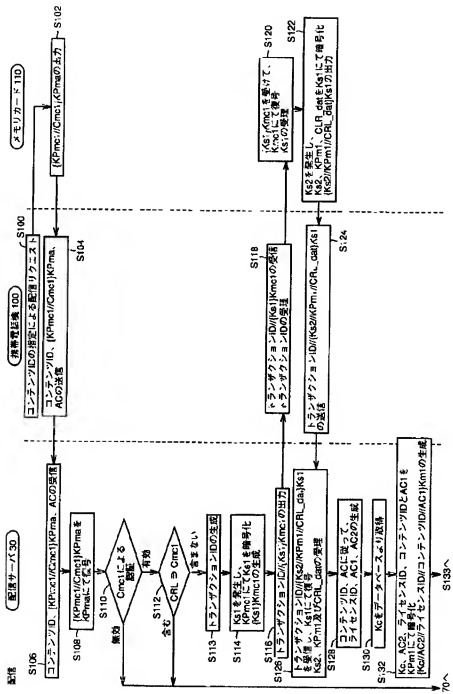
【図９】


記憶サーバ30
携帯電話機100
メモリカード110
開始
S72
コンテンツメニュー送信要求の受信
S70
コンテンツメニュー送信要求の送信
S74
コンテンツメニュー情報の送信
S76
コンテンツメニュー情報の受信と表示
S78
終了
コンテンツ選択
次メニュー
決定
メニュー情報から選択したコンテンツのコンテンツIDを抽出
S80
ライセンスの購入条件ACの入力
S82
S84
選択したコンテンツに対するコンテンツID:C
同一のコンテンツIDを持つ[Data]:Kcが
メモリカード内に記録されていないか検索
S86
選択コンテンツ∈メモリカード
No
S88
Yes
データ取得="Yes"
S90
ライセンスの複製
再生可？
No
Yes
S92
ライセンス再購入
の意思確認
No
Yes
データ取得="No"
S94
終了へ
S100へ

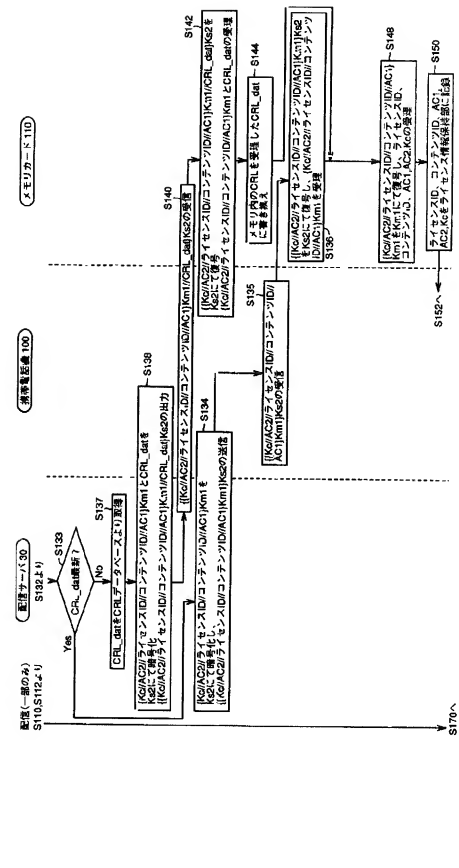
【図１９】


140
142
BS5
コントロ－ラ
ライセンス
保護モジュール
HDD
141
144
パーソナルコンピュータ
130
110
100
メモリカード
ライタ
110

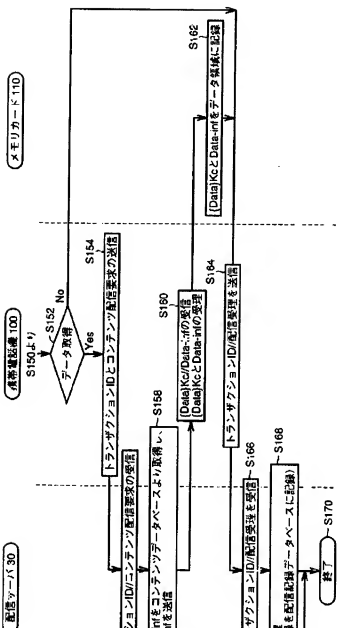
【図10】


配信
配信サーバ130
S106
コンテンツID、{KPcnc1/CdCnc1}KPma、ACGの受信
S108
{KPmc1/CdCnc1}KPmaを{KPmaに}で伝号
S110
Cmc1による認証
無効
有効
S112
CRL ∋ Cmc1
含む
含まない
S113
トランザクションIDの生成
S114
Ks1を乗じ{KPmc1}で{Ks1}を暗号化{Ks1}Kmc1の生成
S116
{トランザクションID//Ks1//Kmc1}の出力
S118
{トランザクションID//Ks1}Kmc1の受信
S120
{Ks1//Cmc1}を乗じて、{Ks1}の算出
S122
Ks2を発生し、CLR_dat{Ks1}にて暗号化{Ks2//KPm1//CRL_dat}{Ks1}の出力
S124
{トランザクションID//Ks2//KPm1//CRL_dat}Ks1の受信
S126
{トランザクションID//Ks2//KPm1//CRL_dat}Ks1を{KPm1//Cmc1}で復号
S128
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S130
Kcをデータベース2に登録
S132
Kc、AC2、ライセンスID、コンテンツIDとAC1を{KPm1}にて暗号化{Kc//AC2//ライセンスID//コンテンツID//AC1}Kmの生成
S136
S170へ
S138へ
メモリカード110
S100
{KPmc1//Cmc1//KPma}の出力
S102
S104
コンテンツID、{KPcnc1//Cmc1}KPma、ACGの送信

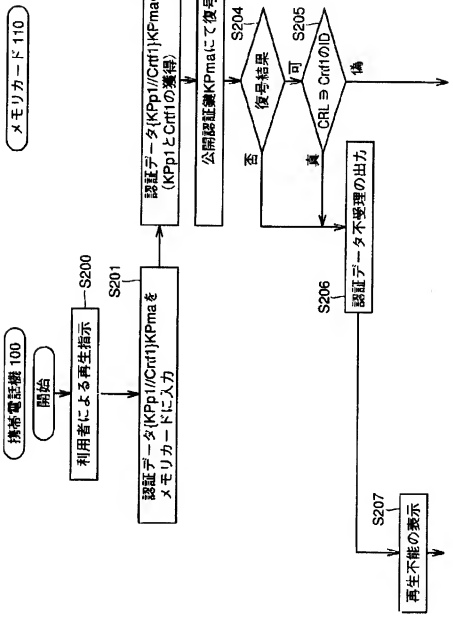
【図11】


配信（一部のみ）
S110,S112より
配信サーバ30
S130より
S133
CRL_dat更新？
Yes
No
S137
CRL_datをCRLデータベースより取得
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'をKci//AC2i//ライセンスID//コンテンツID//AC1]Km1'にて復号
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'をKci//AC2i//ライセンスID//コンテンツID//AC1]Km1'にて暗号化
S139
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とCRL_datをKci//AC2i//ライセンスID//コンテンツID//AC1]Km1'にて暗号化
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とCRL_datをKci//AC2i//ライセンスID//コンテンツID//AC1]Km1'にて暗号化
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とKc2の出力
S134
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とKc2の送信
S135
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とKc2の受信
S140
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とCRL_datとKc2の受理
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とCRL_datをKci//AC2i//ライセンスID//コンテンツID//AC1]Km1'にて復号
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とCRL_datとKc2を{Kci//AC2i//ライセンスID//コンテンツID//AC1}Km1'にて暗号化
S142
メモリ内のCRLを更新したCRL_dat
S144
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'とKc2を{Kci//AC2i//ライセンスID//コンテンツID//AC1}Km1'にて暗号化
S136
[Kci//AC2i//ライセンスID//コンテンツID//AC1]Km1'をKm1'にて復号し、ライセンスID、コンテンツID、AC1,AC2,Kciの受理
S146
ライセンスID、コンテンツID、AC1,AC2,Kciをライセンス格納部に記録
S150
S152へ
S170へ
メモリカード10
通常動作時100

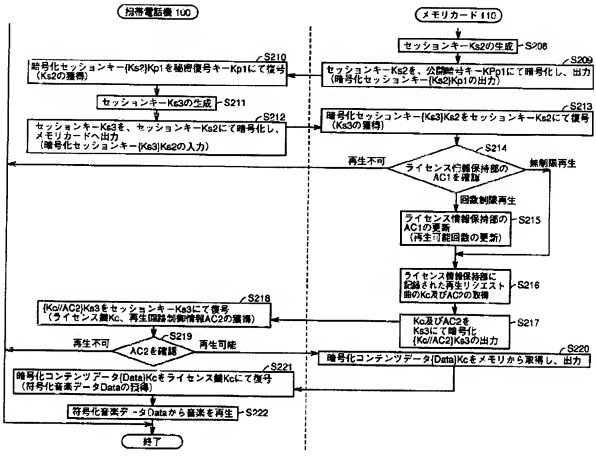
【図12】


配信サーバ30
携帯端末機100
メモリカード110
開始
S150より
S152
データ取得
No
Yes
S154
トランザクションIDとコンテンツ配信要求の送信
S156
トランザクションID//コンテンツ配信要求の受信
S158
[Data]Kcと[Data-inf]をコンテンツデータベースより取得し、
[Data]Kcと[Data-inf]を送信
S160
[Data]Kc//Data-inf]の受信
[Data]Kcと[Data-inf]の復号
S164
トランザクションID//配信要求を送信
S166
トランザクションID//配信要求を受信
S168
終了処理
(配信記録を配信記録データベースに記録)
S170
終了
S166
[Data]Kcと[Data-inf]をデータ領域に記録
終了

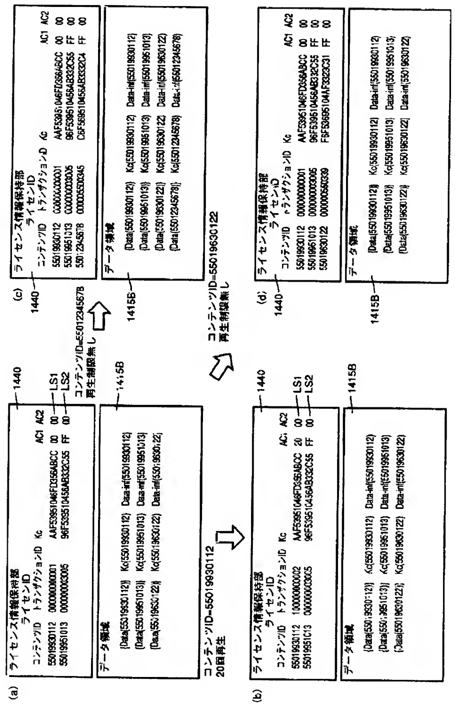
【図15】


携帯電話機 100
メモリカード 110
開始
利用者による再生指示
S200
認証データ{KPp1//Cnt1}KPmaを
メモリカードに入力
S201
認証データ{KPp1//Cnt1}KPmaの受理
(KPp1とCnt1の獲得)
S202
公開認証鍵KPmaにて復号
S203
復号結果
S204
否
真
CRL ∋ Cnt1のID
S205
可
偽
認証データ不受理の出力
S206
再生不能の表示
S207

【図16】


携帯電話機 100
メモリカード 110
セッションキーKs2の生成 S208
S210
暗号化セッションキー{Ks2}Kp1を秘密復号キーKp1にて復号
(Ks2の獲得)
S209
セッションキーKs2を、公開暗号キーKPp1にて暗号化し、出力
(暗号化セッションキー{Ks2}Kp1の出力)
セッションキーKs3の生成 S211
S212
セッションキーKs3を、セッションキーKs2にて暗号化し、
メモリカードへ出力
(暗号化セッションキー{Ks3}Ks2の入力)
S213
暗号化セッションキー{Ks3}Ks2をセッションキーKs2にて復号
(Ks3の獲得)
S214
再生不可
ライセンス情報保持部のAC1を確認
無制限再生
回数制限再生
ライセンス情報保持部のAC1の更新
(再生可能回数の更新)
S215
ライセンス情報保持部に記録された再生リクエスト曲のKc及びAC2の取得
S216
S218
{Kc//AC2}Ks3をセッションキーKs3にて復号
(ライセンス鍵Kc、再生回路制御情報AC2の獲得)
Kc及びAC2をKs3にて暗号化
{Kc//AC2}Ks3の出力
S217
再生不可
S219
AC2を確認
再生可能
S220
暗号化コンテンツデータ{Data}Kcをメモリから取得し、出力
S221
暗号化コンテンツデータ{Data}Kcをライセンス鍵Kcにて復号
(符号化音楽データDataの獲得)
符号化音楽データDataから音楽を再生 S222
終了

【図17】


(a)
ライセンス情報保持部
ライセンID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 000000000001 AAF53951046FD356ABCC 00 00
55019951013 000000003005 96F539510456AB332C55 FF 00
LS1
LS2
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B
コンテンツID=55019930112
20回再生
(b)
ライセンス情報保持部
ライセンID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 100000000002 AAF53951046FD356ABCC 20 00
55019951013 000000003005 96F539510456AB332C55 FF 00
LS1
LS2
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B
コンテンツID=550123456789
再生制限無し
(c)
ライセンス情報保持部
ライセンID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 000000000001 AAF53951046FD356ABCC 00 00
55019951013 000000003005 96F539510456AB332C55 FF 00
55012345678 000005500345 C6F569510456AB3332C4 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
{Data(55012345678)} Kc(55012345678) Data-inf(55012345678)
1415B
コンテンツID=55019630122
再生制限無し
(d)
ライセンス情報保持部
ライセンID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 000000000001 AAF53951046FD356ABCC 00 00
55019951013 000000003005 96F539510456AB332C55 FF 00
55019630122 000000560339 F6F53695104AF3323C31 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B